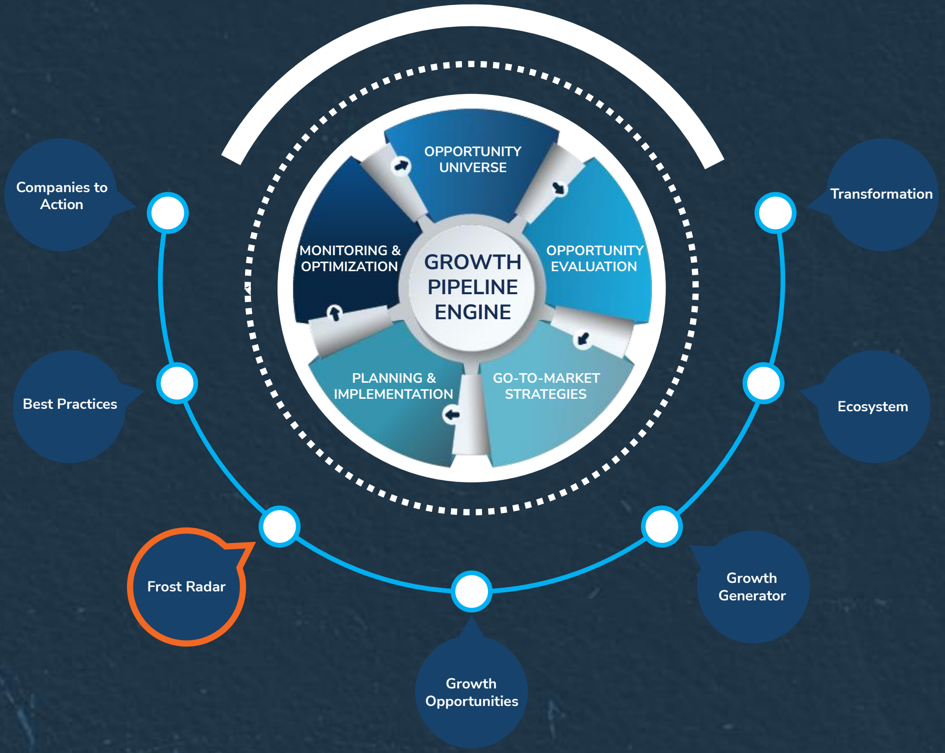
FROST & SULLIVAN

Frost Radar™: Automated Security Validation, 2026

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



Authors: Daphne Dwiputriane and Ying Ting Neoh
Contributors: Swetha Krishnamoorthi and Jarad Carleton

PG6U-74
February 2026

Strategic Imperative and Growth Environment

List of Abbreviations

- **AI:** Artificial Intelligence
- **API:** Application Programming Interface
- **APT**: Autonomous Penetration Testing
- **ASM:** Attack Surface Management
- **ASV:** Automated Security Validation
- **BAS:** Breach Attack Simulation
- **CAGR:** Compound Annual Growth Rate
- **CEM:** Continuous Exposure Management
- **CSP:** Cloud Service Provider
- **CTEM:** Continuous Threat Exposure Management
- **CNAPP:** Cloud-Native Application Protection Platform
- **CVE:** Common Vulnerabilities and Exposures
- **CVSS:** Common Vulnerability Scoring System
- **EASM:** External Attack Surface Management
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **GenAI:** Generative AI
- **GTM:** Go to Market
- **GSI:** Global System Integrator
- **IaC**: Infrastructure as Code
- **ICS**: Industrial Control System
- **IoT:** Internet of Things
- **ITSM:** IT Service Management
- **K8s:** Kubernetes
- **LLM:** Large Language Model
- **MCP:** Model Context Protocol
- **ML:** Machine Learning
- **MSP:** Managed Service Provider
- **MSSP:** Managed Security Service Provider
- **OT**: Operational Technology
- **OWASP:** Open Worldwide Application Security Project
- **RBVM**: Risk-Based Vulnerability Management
- **RemOps**: Remediation Operations
- **RTAP:** Red Teaming Automated Platforms
- **SaaS:** Software-as-a-Service
- **SecOps:** Security Operations
- **SIEM:** Security Information and Event Management
- **SME**: Small and Medium-Sized Enterprises
- **SOAR:** Security, Orchestration, Automation and Response
- **SOC:** Security Operations Center
- **SSCS:** Software Supply Chain Security
- **SSPM:** SaaS Security Posture Management
- **TTP**: Tactics, Techniques, and Procedures
- **XDR:** Extended Detection and Response

Source: Frost & Sullivan

Strategic Imperative

- In recent years, enterprises across the globe have transformed how they operate, driven by the adoption of cloud-native technologies, cloud computing, SaaS applications, K8s, APIs, and AI/ML. While this has unlocked significant revenue growth and operational agility, it has expanded the enterprise attack surface and exposed the limitation of traditional, point-in-time penetration testing models.
- Security programs in these dynamic environments have shifted toward more continuous and automated approaches that enable enterprises to proactively identify vulnerabilities and exposures earlier, but it has also contributed to alert overload as more issues are surfaced without clear context on exploitability. Consequently, enterprises are recognizing the need to distinguish between theoretical weaknesses and those most likely to be exploited in real-world attacks.
- This has positioned ASV as a necessity rather than an option because its emphasis on validation effectively shifts the security conversation from hypothetical risk to validated, evidence-based risk. In general, an ASV solution continuously tests and validates the effectiveness of an enterprise's security controls, allowing enterprises to prioritize remediation based on evidence and ensure that controls are effective in a continuously evolving threat landscape.
- As ASV solutions have matured, they have evolved into a set of complementary subsegments—APT, RTAP, BAS, and CEM—that individually address different layers of the validation problem from exposure discovery to control validation but are unified by a common security outcome of continuously validating security effectiveness in real-world situations.

Source: Frost & Sullivan

Strategic Imperative (continued)

- By correlating findings across these subsegments within a single console, ASV platforms integrate exploitability validation, real-time threat intelligence, and control effectiveness checks to determine which exposures pose the highest risks. Together, the subsegments form the executional layer for modern CTEM programs. CTEM is a framework that has an increasing influence in guiding ASV adoption because it helps enterprises define how they can discover exposure, validate which exposure matters, prioritize remediation, and perform these tasks continuously to ensure security resilience.
- Several trends are shaping the evolution of the ASV market. The broader adoption of agentic AI is redefining many cybersecurity solutions, including ASV, because it enables more contextual, predictive and autonomous workflows. Attack simulations can dynamically adapt based on real-time context while policy-bounded autonomous agents can create a dynamic feedback loop between validation and mitigation to support continuous improvement.
- ASV solutions are also increasingly expected to translate technical findings into business metrics by incorporating effectiveness of security controls into exposure scores, enabling CISOs to align security investments with measurable outcomes. At the same time, ASV platforms are becoming more tightly integrated into SecOps workflows, which streamline remediation by validating exploitability and enabling faster, evidence-driven response through integrations with an existing security stack.
- As the ASV market continues to evolve across the four overlapping subsegments, vendors can enter the space through different anchor use cases aligned with their core strengths, supplementing them with adjacent capabilities. While this has lowered entry barriers and diversified innovation, it has also intensified competition and diluted differentiation. To stand out, ASV vendors must continue evolving toward tightly integrated platforms that deliver end-to-end visibility and continuous risk reduction.

Source: Frost & Sullivan

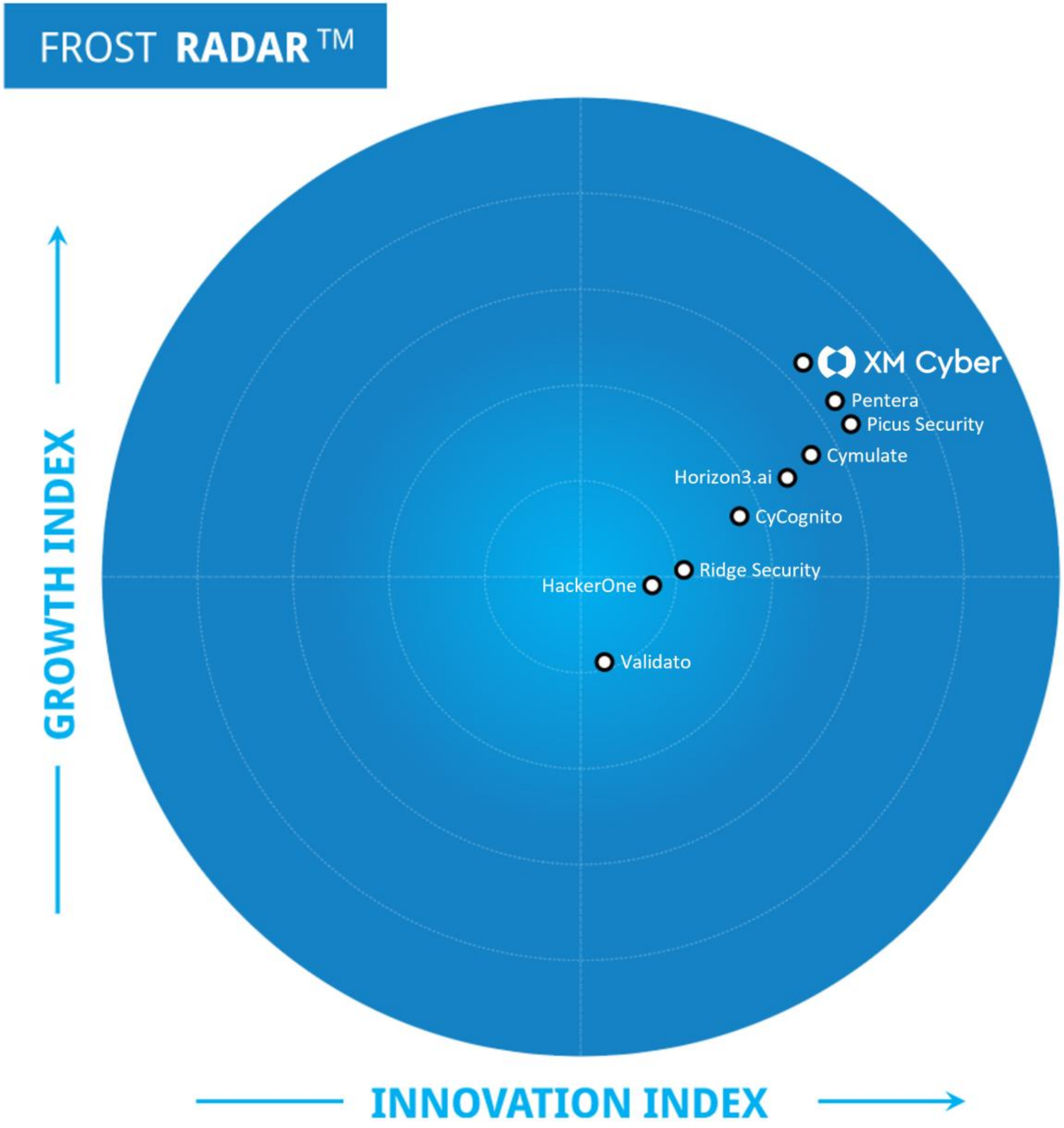
Growth Environment

- The market's 47.2% growth rate in 2025 indicates that ASV is becoming a highly recognizable category with enterprises increasingly willing to pay for validation to show strong proof that their controls work. Its CAGR for the 2025–2030 period is anticipated to be 24.8%, signaling steady growth opportunities because of an increasing threat landscape that would require enterprises to purchase solutions to validate controls and provide attack-path analysis to identify blind spots before they can be exploited.
- Growth is fueled by the combined momentum of four subsegments that aim to achieve the same outcome. This creates demand across multiple, use-case-driven entry points because enterprises are adopting ASV capabilities based on their specific risk priorities and readiness levels.
- North America leads in the adoption of ASV. Security teams in the region tend to be more mature and determined to reduce the attack surface area because they are often at the forefront of adopting the latest technologies, exposing them to the greatest risk. EMEA is a close second as regulations including GDPR and the DORA Act require enterprises to demonstrate evidence that their security controls are effective. Latin America and Asia-Pacific contribute considerably less revenue but will grow at a significantly faster rate as awareness of the solutions continues to grow.
- Very large (at least 5,000 employees) and large (1,000 to 4,999 employees) enterprises contributed the most revenue to the ASV market globally in 2025 and are expected to remain the largest contributors until 2030 because their more complex security needs result in higher-value deals. BFSI, technologies and telecommunications, and manufacturing are the primary sectors contributing to ASV revenue.

Source: Frost & Sullivan

Frost Radar™: Automated Security Validation

Frost Radar™: Automated Security Validation



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- From more than 20 participants in the space, Frost & Sullivan shortlisted nine Growth and Innovation leaders for this Frost Radar™ analysis based on a minimum estimated annual revenue threshold of $1 million in 2025. At its core, the ASV market is composed of a diverse set of vendors that specialize in BAS, RTAP, APT, or CEM but are converging around a shared goal of helping enterprises validate security controls, identify exposures, and prioritize remediation through continuous testing. This ensures that existing controls remain effective in an ever-evolving threat landscape.
- Rather than forming separate categories, the market exists as a spectrum of approaches. Some vendors emphasize APT and BAS; some operate at the intersection of RTAP and BAS while leveraging crowdsourced ethical hacking to uncover vulnerabilities; some focus on unified visibility and attack path analysis; some combine APT with risk-based validation to align remediation with operational priorities.
- As the market converges around a common goal, differentiating vendors becomes challenging. Each brings unique specialties and often supplements them with adjacent capabilities. For this reason, Frost & Sullivan evaluates vendors not only on their ability to deliver the core ASV goal, but also their advancement in areas such as correlating findings from multiple subsegments in a single console; seamless integration into SecOps workflows; use of agentic AI to orchestrate validation tasks as well as real-time dashboard reporting and recommended remediation actions based on business impact; risk quantification in business terms; and inclusion of offensive security for AI ecosystems.
- Ultimately, differentiation is subtle because most vendors can address the core validation needs. The key distinction now lies in how effectively a vendor leverages historical strengths while extending capabilities to deliver coherent, measurable operational outcomes. For enterprises, selecting the right vendor depends less on ticking off a feature checklist and more on finding an ASV solution that addresses their most urgent security needs and matches their budget.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- XM Cyber is the Frost Radar^{TM} Growth Index leader, driven by a combination of expanded GTM execution and its ability to leverage its parent company's broad customer base for access to large, regulated enterprises, driving adoption of its flagship platform globally. XM Cyber is also well placed on the Innovation Index because of its platform's comprehensive coverage, with the Choke Point Analysis feature as a strong differentiator for effectively collapsing complex attack paths into a small set of high-impact remediation actions.
- Pentera, Picus Security, and Cymulate are Growth Index standouts and Innovation Index leaders. These vendors have demonstrated consistent financial strength over the past three years, marked by revenue and market share growth in the global ASV market, while also signaling strong future potential through their roadmaps and forward-thinking GTM strategies. Core capabilities underpin their market leadership: emulating real-world attacks, validating security controls, and identifying exploitable weaknesses. They deliver platforms that ensure that their capabilities are aligned with the latest adversary tactics, while prioritization features help security teams focus on high-impact vulnerabilities, driving measurable improvements in cyber resilience.
- Horizon3.ai enters the ASV market from an APT-first foundation rooted in a real attacker mindset. Its NodeZero platform simulates real-world attacks at scale to help enterprises identify and mitigate exploitable vulnerabilities before attackers can leverage them. The company has been actively expanding its platform capabilities, and a recent $100 million funding round strengthens its ability to accelerate product innovation and global GTM execution.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- CyCognito approaches ASV from an external attack surface-centric perspective, leveraging its deep expertise in external asset discovery and exposure mapping. By pairing comprehensive external discovery with contextual risk intelligence, the platform prioritizes exposures based on exploitability and an ability to chain into meaningful business impact, making it particularly relevant for enterprises concerned with outside-in and lateral attack scenarios.
- HackerOne anchors its approach in human-in-the-loop validation and crowdsourced adversarial testing and is augmenting this model with automation and AI to improve scalability and operational efficiency. This positions the company as an option for enterprises that prioritize human expertise and realism, particularly in highly regulated and sensitive industries.
- Ridge Security, by contrast, emphasizes agentless APT and adversarial emulation at a more accessible price point. This pricing and delivery model allows the company to position itself as a viable alternative for small and midsize enterprises that are often priced out of enterprise-centric ASV offerings but still seek meaningful validation capabilities.
- Validato earns its place on the Frost Radar™ through strong compliance alignment, accessibility for midsize enterprises, and a focused, pure-play approach to security validation. Compared to market leaders, the company needs to be clearer in articulating its differentiated long-term roadmap or demonstrate the scale and geographic reach needed to compete at the highest tier of the ASV market.

Source: Frost & Sullivan

Frost Radar™: Companies to Action

XM Cyber

INNOVATION

- XM Cyber's presence in the ASV market is rooted in its flagship Continuous Exposure Management (CEM) platform, which provides a unified view of an enterprise's entire attack surface and the way that exposures interconnect into viable attack paths. Rather than presenting exposures in isolation, XM Cyber shows how attackers can realistically traverse hybrid environments to reach critical business assets.
- The XM Cyber platform supports on-premises, multicloud, and hybrid environments, mapping how attackers can move laterally across external-facing systems, cloud workloads, identity infrastructure such as Active Directory, and K8s environments. In response to emerging enterprise realities, the company is expanding its coverage to address AI-related attack surfaces driven by GenAI adoption as well as planning support for increasingly interconnected OT environments.
- At the core of the CEM platform is XM Attack Graph Analysis™, which models all possible paths an attacker could take through an enterprise's environment. While attack graphs have become common across the ASV market, XM Cyber differentiates through its Choke Point Analysis, which collapses complex exposure data into a smaller number of actionable remediation efforts. By identifying security controls that can disrupt multiple attack paths simultaneously, this exploitability-centric prioritization helps enterprises maximize risk reduction per remediation action and significantly reduce operational workload.
- XM Cyber further differentiates through its use of a digital twin, which enables attack path validation and exposure testing without executing live exploits in production environments. This approach minimizes operational risk while maintaining high-fidelity security insights, making it particularly attractive to risk-averse industries, such as financial services and critical infrastructure.

Source: Frost & Sullivan

XM Cyber (continued)

INNOVATION

- Following its acquisition by Schwarz Digits in 2021, XM Cyber's platform is available on STACKIT, Schwarz Digits' sovereign cloud platform, operating under strict EU data protection and compliance requirements. Given that ASV platforms often ingest highly sensitive infrastructure and identity data, this deployment option lowers adoption friction for European enterprises and government institutions that have reservations about US hyperscalers. As a result, XM Cyber is well positioned among customers with stringent data residency and sovereignty requirements.
- To strengthen its platform, XM Cyber has released several enhancements, including sensorless risk measurements for legacy environments, passive scanning capabilities, customizable executive reporting, and cross-environment attack graph reporting. These additions build on its core strength in attack path analysis while supporting broader enterprise use cases. Its roadmap also highlights investments in third-party integrations, cloud and identity security coverage, and AI-related exposure analysis.
- In line with the broader market trend, XM Cyber is leveraging GenAI to support security analysts and reduce operational friction. The company introduced Ask XM, a natural-language interface that allows analysts to query the platform for deeper insights and faster analysis. XM Cyber also is developing AI agents designed to act as intelligent advisors, proactively identifying choke points and recommending remediation actions to streamline analyst workflows and accelerate decision-making.

Source: Frost & Sullivan

XM Cyber (continued)

GROWTH

- XM Cyber is the Growth Index leader on the Frost Radar™ thanks to its expanding global footprint, diversified customer base, and a growth rate that remains in line with the overall ASV market. This momentum is reflected in its ability to quadruple its total contract value over the past four years.
- The company has effectively leveraged the broad customer base of its parent company to deploy its ASV platform across sectors including banking, technology and telecommunications, and manufacturing. Because of its German-based parent company and strong presence in Europe, EMEA was the largest contributor to XM Cyber's ASV revenue in 2025. The company has also built a considerable presence in North America, Latin America, and Asia-Pacific.
- XM Cyber offers relatively straightforward pricing based on the number of assets under management. Predictable pricing helps customers avoid unexpected cost increases as environments scale. Customers can add modules, such as EASM and Exposed Credentials Management, when needed, allowing them to address immediate priorities while maintaining pricing flexibility.
- XM Cyber's Exposure Management Service helps security teams translate prioritized exposure insights into action. The service allows XM Cyber to help customers track remediation progress and operationalize exposure management more effectively in their security workflows. It helps close the execution gap between exposure discovery and risk reduction, ensuring that identified risks are actively reduced over time rather than just being surfaced.

Source: Frost & Sullivan

XM Cyber (continued)

FROST PERSPECTIVE

- XM Cyber is a leading player in the ASV market, anchored by its flagship CEM platform that provides an interconnected, attacker-centric view of the full attack surface—all modeled in a digital twin to safely simulate attack paths without impacting production. Its Choke Point Analysis is a differentiator that helps to reduce remediation workload and ensures that enterprises can focus on high-impact actions by identifying security controls that can disrupt multiple attack paths simultaneously.
- As the platform continues to expand its use cases, XM Cyber will need to ensure that increased breadth does not come at the cost of operational manageability or customer complexity. Maintaining a cohesive platform experience with stronger integration and prioritization support while deepening analytical depth around interconnected exposures will be important to preserve usability at scale.
- Expanding real-world exploitability validation for emerging attack vectors, such as GenAI-related exploits that include prompt leakage and model misuse, would strengthen remediation decision-making. More targeted automated penetration testing for high-risk paths identified through attack graph could enhance its ability to perform more high-impact remediation. Deeper exploitability testing and tailored attack scenarios for other emerging domains, such as AI/ML workloads and OT exposures, would also enhance remediation decision-making.
- XM Cyber has effectively leveraged its parent company's customer base, but long-term growth will require a more aggressive GTM strategy beyond inherited channels. The company also will need to sharpen its platform narrative, whether it aims to position itself as comprehensive CTEM- and ASV-led platform or expand into adjacent domains, such as EASM. While these domains are increasingly interconnected, pursuing them at scale would require investments to be adjusted accordingly across product development, marketing and ecosystem strategy, which might affect its long-term momentum.

Source: Frost & Sullivan

Best Practices & Growth Opportunities

Best Practices

1 CISOs should adopt ASV solutions that unify BAS, APV, and ASM or integrate with VM, XDR, and SOAR to reduce sprawl. These platforms must provide centralized visibility across assets and attack paths while mapping vulnerabilities to critical business processes. By adjusting attack paths based on live context, organizations can move beyond static testing to achieve proactive exposure management.

2 To combat alert fatigue, ASV platforms should integrate with SecOps workflows and threat intelligence while providing automated, audit-ready evidence aligned with NIS2, DORA, SEC rules, and the EU AI Act. They must offer continuous monitoring, regulator-friendly reporting, and automated compliance attestations to replace manual processes. Platforms should quantify risk by financial impact, regulatory exposure, and operational disruption, ensuring that remediation targets critical business priorities.

3 The ideal ASV vendor aligns with organizational priorities (including scalability), seamlessly integrates with existing security infrastructure, and offers strong compliance capabilities and proactive support for customer success. Vendors should also demonstrate a clear roadmap and innovation strategy that adapts to emerging risks and regulatory requirements, ensuring long-term effectiveness and relevance.

Source: Frost & Sullivan

Growth Opportunities

1. ASV vendors should position CEM as their core value proposition, replacing fragmented manual processes with unified workflows for discovery, validation, and prioritization. Whether through native integration, strategic partnerships, or M&A, vendors must build a single-pane-of-glass platform interoperable with ASM, RBVM, and digital risk protection services. Investments should focus on extending visibility across hybrid environments, multicloud, OT, and AI exposures while delivering a seamless user experience.

2. Agentic AI, GenAI, and ML capabilities are imperative for real-time find-fix-verify workflows, compliance evidence generation, and guided playbooks. Vendors should leverage structured reasoning architectures combining graph-based search, LLM reasoning, and deterministic exploitation to automate analytics, reporting, and remediation. Prioritizing AI-specific test suites for model-aware threats and validation aligned with certifications such as ISO 42001 would future-proof compliance and secure enterprise AI environments.

3. ASV vendors should develop robust partner programs with MSSPs and GSIs to deliver co-managed and fully managed services. This includes multitenancy for MSSPs, localized go-to-market support, and marketplaces for frictionless procurement and co-sell motions. By embedding ASV capabilities into SecOps workflows and cloud ecosystems, vendors can accelerate adoption, track measurable improvements in security posture, and position themselves as trusted partners for enterprise resilience.

Source: Frost & Sullivan

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar^{TM}.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Source: Frost & Sullivan

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGA TRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com